

Advanced Communications Project

Shipboard Communications Center Intelligent Gateway Demonstration Report

Prepared for
**The United States Coast Guard
Research & Development Center
1082 Shennecossett Rd.
Groton, CT 06340-6096**

By
**PRC Inc. and
VisiCom Laboratories Inc.**
Via
Volpe NTSC



March 1995

Table of Contents

1.0 INTRODUCTION & SCOPE	1
2.0 BACKGROUND	1
3.0 APPLICABLE DOCUMENTS	4
3.1 Government Documents	4
3.2 Non-Government Documents	4
4.0 GATEWAY TECHNICAL SUMMARY	5
4.1 Introduction	5
4.2 SCE Implementation Approach	5
4.3 CSS SCE Overview	7
4.4 Fielded/Planned SCE Implementations	9
5.0 DEMONSTRATION CONFIGURATION	14
5.1 JOTS	14
5.2 LEDS	15
5.3 Traffic Generator	15
5.4 Gateway Element (CSS SCE)	15
5.5 Link Access Elements	15
5.6 KG-84A	16
5.7 MX-518 Modem	16
5.8 TD-1271	16
6.0 DEMONSTRATION OVERVIEW	16
Appendix A Prototype CSS SCE Routing Algorithm	18
Appendix B Acronyms	20

Figures

Figure 1. SCE Architecture.....	8
Figure 2. NAVMACS Front End Processor	10
Figure 3. NAVMACS MODEL II.....	12
Figure 4. NECC Block Diagram.....	13
Figure 5. CSS SCE Demonstration Configuration	14

1.0 INTRODUCTION AND SCOPE

The United States Coast Guard Research and Development Center (R&D Center) has a requirement to modernize and improve communications centers on Coast Guard cutters. The USCG R&D Center teamed with the Volpe Center to evaluate requirements in the radio rooms of various classes of Coast Guard Cutters in order to improve communications capabilities on these vessels, as current USCG cutter communications centers are manpower intensive and require a multi-person watch. This effort is analogous to the COMMSYS 2010 project, which is investigating ways to modernize the USCG shoreside communications infrastructure. In support of this cutter modernization effort, a prototype shipboard intelligent gateway was demonstrated to the Coast Guard at the Naval Command, Control and Ocean Surveillance Center, Research Development and Test Evaluation Division (NRaD) on February 1, 1995. The demonstrated gateway is based upon the Communication Support System (CSS) Standard Communications Environment (SCE). This system performs automated routing of message data and permits different communication user systems (e.g., Link-11, JOTS, NAVMACS) to share radio frequency (RF) media. It is a technology based upon the use of commercial standards and products, features a scalable and open architecture, and is undergoing deployment in U. S. Navy systems today. It appears to be a strong candidate for both the conceptual and implementation basis for a U.S. Coast Guard Cutter Intelligent Gateway.

The demonstration was performed by Visicom Laboratories, under subcontract to PRC Inc.'s contract with the Volpe Center. This report provides a technical overview of this gateway. The report focuses primarily on the architectural design and philosophy of the gateway and its utility as the framework for U.S. Navy and U.S. Coast Guard afloat communication architecture.

2.0 BACKGROUND

The CSS is intended to be the aggregate Navy capability to provide radio frequency information exchange services to a wide variety of US Navy information consumers. The CSS concept was formulated to provide a greater degree of survivability and efficiency in the manner that the Navy allocates and uses its communications resources. This concept is also directly applicable to the Coast Guard as it pertains not to specific systems and applications but rather to a communications framework. This framework has already been developed, studied and analyzed in great detail, and has reached a maturity level such that it is now in the process of being introduced seamlessly into operational Navy platforms. Implementing this gateway technology into Coast Guard cutters would involve integration rather than costly development of an architecture and technology currently undergoing field testing.

The consumers in today's Coast Guard communications environment exchange data and voice information via dedicated semi-permanently assigned circuits. The consumers are located upon mobile platforms such as cutters and aircraft and ashore at communications stations. The stations ashore act as gateways between shore based commands and installations (accessed via global land based communications networks) and the Coast Guard's mobile platforms at sea. Each communications path is associated with a specific data link and network protocol, a fixed frequency assignment, specific radio, modem, and encryption equipment, unique data formats, and a dedicated set of consumers. These consumers are known as "users". The users are Coast Guard personnel or computer systems which have a requirement to exchange text, voice, and computer to computer data. The protocols developed for each of these communications paths were accomplished in accordance with the requirements and funding limitations of each user group. No consideration was given to multiple user groups sharing pooled frequencies.

An example of such a user group or user community of applicability to the Coast Guard is that group (NAVMACS) involved with the Common Users Digital Information Exchange Subsystem (CUDIXS) of the Navy Fleet Satellite Communications System (FLTSATCOM). This is dedicated to the exchange of formal General Service (GENSER) record messages. A record message is a formatted text oriented element of information to be exchanged between commands. The transmission of a record message must be approved by the commander at the source site and thus represents information that is for the "record". These messages specifically address actions and performance of tactical or administrative nature. The CUDIXS is allocated to a single 25 kHz UHF satellite channel providing broad earth coverage. Five satellites make up the entire constellation with at least one channel on each satellite used for CUDIXS. The CUDIXS equipment includes processors, encryption equipment, modems, radios and antennas. Each station has nearly identical processing capabilities for CUDIXS data exchange. Each station uses the same access protocols, network protocols, and data link protocols.

This dedicated resource approach has the advantage that it is relatively easy to identify and specify the communications requirement, and the system is relatively isolated from faults in other Navy communications system components. On the other hand there is no tolerance for any major faults involving failure of any system components. Similarly, where there are failures in other systems, there is no ability to use the inherent communications capability of CUDIXS for the exchange of other kinds of information. Similarly, CUDIXS is incapable of using other communications media such as HF, EHF, or SHF.

In order to provide more efficient use of the available bandwidth, provide additional user access and increase the reliability and survivability of the Navy's communications networks, the Navy has developed the CSS concept and technology. By providing an overall architecture in which

systems can be integrated, implementation costs are minimized and message delivery performance is maximized.

The proposed CSS architecture, afloat and ashore, has extraordinary impacts upon existing and planned programs. The CSS architecture permits a greater degree of communications functionality for existing and planned systems without any significant cost burden. This is made possible by integrating the efforts of all of the user communities in their efforts to increase their communications capability within the CSS architectural framework. This permits the "products" of individual programs to be made available to other programs. The CSS framework allocates the individual RF resources across all of the user systems.

To achieve an integrated capability, the architecture specifies RF communications link processors decoupled from the user systems. The users are essentially provided a standard "black box" interface to the **entire** RF communications suite. The CSS architecture provides for connectivity to multiple radio frequency bands. Each user can be allocated multiple resources. These protocols will permit the user to approach the communication system as a pool of resources available to effect data transfer to and from other platforms. This system will automatically route message data without any human intervention. As far as the producer of the message is concerned, the message was transmitted to the destination. This is evidenced by the receipt of a delivery status message as specified by the user. The message producer is completely de-coupled from the communications equipment. Additionally, the system will, as a result of this architecture and the embedded protocols, be capable of providing more timely and more accurate data transfer across a broad range of operational environments.

3.0 APPLICABLE DOCUMENTS For additional detail and background information, the reader of this report is directed to the following specified documents.

3.1 Government Documents

Naval Command, Control and Ocean Surveillance Center, Research Development and Test Evaluation Division (NRaD):

System Specification Document for the Communications Support System (CSS), CSS-A001BA-SSSb-(D)-042991, 29 April 1991. *This document specifies the U.S. Navy's CSS of which the prototype SCE, the router demonstrated for the U.S. Coast Guard on February 1, 1995, is described in relation to the overall communications architecture being implemented for the U.S. Navy.*

EOC-II System Test Plan (STP), 1 December 1994 [DRAFT]. *This document is the only formal documentation existing which describes the NRaD test site at which the demonstration occurred. It describes the hardware - both baseband and RF - which was employed for the demonstration.*

3.2 Non-Government Documents

International Standards Organization (ISO):

ISO 7498 Information Processing Systems - Open Systems Interconnection - Basic Reference Model, 15 October 1984. *This document defines the open, layered abstraction for communication systems. It is the foundation upon which all modern communication systems, including those of the Department of Defense , are based.*

4.0 GATEWAY TECHNICAL SUMMARY

4.1 Introduction

The prototype gateway was demonstrated by VisiCom Laboratories on February 1, 1995 at NRaD. It uses data content and the associated delivery requirements of messages (e.g., data precedence, perishability, security requirements, emission control (EMCON) requirements, etc.) to automatically select and route user message data to the computed "optimal" communication resource (medium). This gateway was based on the Communication Support System (CSS) Standard Communications Environment (SCE) prototype software and hardware. The CSS is the implementation of the so-called TADIXS pillar of the U.S. Navy's COPERNICUS architecture and, consequently, all fleet RF communications. The TADIXS are a series of afloat virtual networks of variable duration. Durations are dependent on the information exchange load. They are not communication circuits, but rather information networks sharing communications circuitry over a broad range of communication services ranging from military circuits (HF, VHF, UHF, SHF, and EHF) to those provided by commercial satellites. The demonstrated intelligent gateway was based on the SCE prototype software developed by VisiCom Laboratories, Inc., under contract, to NRaD.

4.2 SCE Implementation Approach

The CSS SCE employs an open system architecture based on commercial-off-the-shelf (COTS) and Non-Developmental Item (NDI) technologies. This open architecture approach is based on the design and development of scalable communication systems built from modular components. The primary motivation in pursuing such an approach is the recognition that complex communications systems cannot be developed and deployed with traditional full-scale development methods within the required time frame and simultaneously achieve all operational, engineering and programmatic goals and requirements. The CSS SCE approach employs NDI components to build a system which meets specific platform (i.e., cutter) requirements without the expense and risk associated with a typical full-scale engineering development effort. It is driven by DoD-wide "re-engineering goals" characterized by:

- Implementing open systems technology
- Maximizing the use of COTS
- Using state-of-the-art processor technology with the built-in mechanism to utilize the technology as it advances

- Installing smaller and lighter hardware suites
- Minimizing maintenance costs and improving reliability
- Scoping Integrated Logistical Support (ILS) activities to meet the specific requirements for support of NDI products.
- Decreasing training costs
- Avoiding "reinventing the wheel"

This approach provides the Coast Guard with the advantages of reduced cost and development risk, while providing long term benefits of reliability, flexibility and growth that extend throughout the operational life cycle of Coast Guard cutters.

The CSS SCE gateway is constructed from an integration of NDI components within an open architectural framework. This implementation is based upon modern software and hardware engineering concepts successfully employed in various U.S. Navy communication programs. This approach ensures that the Coast Guard can install systems today that are survivable in terms of equipment failures and future requirements/technology growth. It permits modular system development, reconfiguration, and incremental expansion, and permits system definition and development using standards available in the public domain. This open systems solution has the following attributes:

- Uses proven NDI hardware and software to fulfill communication requirements.
- Utilizes well published interfaces, such as Ethernet, VME, and SCSI.
- Encapsulates non-standard and non-conforming NDI items with open interfaces through the use of NDI support services.
- Employs modern software engineering concepts, such as information hiding, loose coupling, structured languages (e.g., Ada) and layered software to provide scalability.

This design specifically addresses the Coast Guard concern of utilizing NDI components obsolete at the time of production and operation. This concern must be considered in initial design and can only be reliably addressed through a true open architecture. It is important to note that not all NDI solutions are open. The single key factor in open systems architecture is the definition, management, and communication of standards that specify interfaces, services and supporting formats for interoperability of software and hardware systems and the components of

the systems. For example, older DEC VAX architecture computers would be NDI, but not open because they do not use open (internal) interfaces that allow for interoperability with non-VAX components. To a slightly less degree, the same can be said about the standard Coast Guard workstation. Likewise, the U.S. Navy's standard computers (UYKs) have very closed architecture, but are certainly NDI.

The key benefit of employing an open system architecture is the simplified integration of systems and components not native to the developed system. This benefit is realized in integration, but is even more evident during the product life cycle as system upgrades are made to accept new technologies or to replace outdated equipment. The use of open system standards in NDI can result in reduced development engineering and transition-to-production costs.

4.3 CSS SCE Overview

The SCE is the key component of the Communications Support System (CSS). The CSS architecture provides the basis for the development of future communications systems by establishing standard interfaces between the users of the communications systems and the communications equipment. The CSS architecture specifies communications system standards which permit access by many users to multiple shared-access communications media. Decoupling the user from the communications systems, provides the user with access to multiple media and enhances system survivability from communications jamming and equipment failures.

The CSS Architecture is divided into three primary components: users, the CSS Standard Communications Environment (SCE), and the Link Access Control (LAC) as illustrated in Figure 1 below.

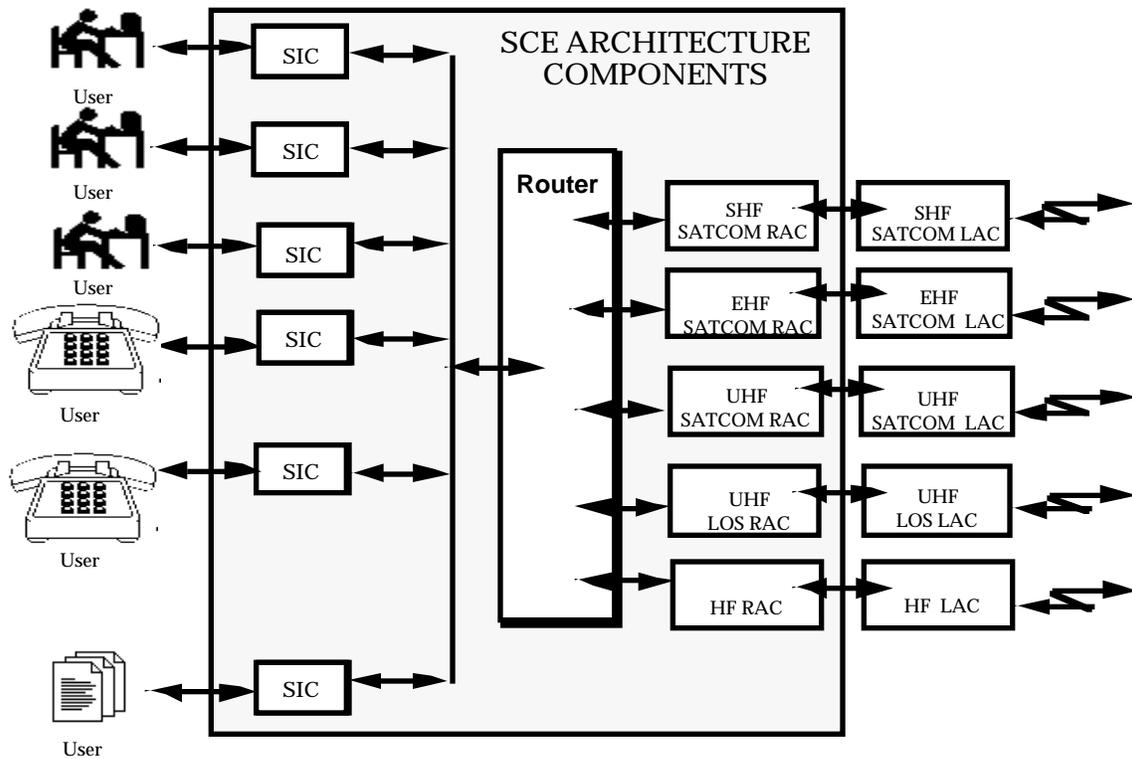


Figure 1. SCE Architecture

The CSS SCE provides the interface between the users and the communications resources controlled by the LAC. Each user determines the communications requirement (i.e., intelligent automated routing). The SCE accepts data from each user and selects the resources required to satisfy that requirement. The SCE consists of three components:

- the Subscriber Interface Control (SIC) - which implements the interface between a specific user and the SCE. Each SIC provides an interface between a specific user and the SCE. A SIC performs the following functions:
 1. convert unique user interfaces to a standard SCE interface,
 2. convert from unique user addressing formats to a standard SCE addressing format,
 3. maintain backward compatibility to existing communications systems.
 4. Some SICs may provide the following additional functions:
 - a. local user to SCE flow control,

- c. data compression and,
 - d. conversion to common external data representation
- the Router - which performs the actual routing of user data to the appropriate RF media. The specific routing algorithm is defined by the system implementor of the CSS framework. It may range from a simple static-table-driven scheme to a complicated expert system;
 - the Resource Access Control (RAC) - which provides for the transfer of user data to other platforms via RF media;

The LAC consists of the specific media used to communicate, the modem and radio equipment employed on this medium, and the subnetwork protocol used to control data exchange over the medium. The LAC applies the necessary resource unique subnetwork and data link protocols necessary to control the exchange via the medium. Thus, the LAC is the hardware and software which provides:

- an interface to the link level encryption,
- the modem,
- encoding/decoding,
- multiplexing,
- radio, and
- antenna.

4.4 Fielded/Planned SCE Implementations

The CSS SCE has been successfully implemented in a number of operational U.S. Navy IXS programs. From the perspective of the U.S. Coast Guard, the most significant fielded implementation is probably the Navy Modular Automated Communication System (NAVMACS), Model II (NAVMACS-II).

There are three components of NAVMACS-II. These components are the Message Processor (MP), the Communications Controller (CC), and the Front End Processor (FEP). The CC was the first fielded implementation of the CSS SCE.

The baseline FEP operates with a KG-36 and supports either a 2400, 4800 or 9600 bps (non-multiplexed) or a 2400 or 4800 bps (DAMA) CUDIXS link. The baseline FEP is hosted on three VME boards and uses serial interfaces to NAVMACS V(5) and the CUDIXS link. The enhanced FEP can operate with a KG-84A, (although none of the U.S. Navy ships on which the system is installed currently have KG-84As). Figure 2 illustrates the baseline and enhanced FEP. The enhanced FEP board set is the same as the baseline FEP board set except that a 68040 microprocessor is used instead of the 68030 microprocessor. The enhanced FEP uses the same data rates and modes (non-DAMA/DAMA) as the baseline FEP.

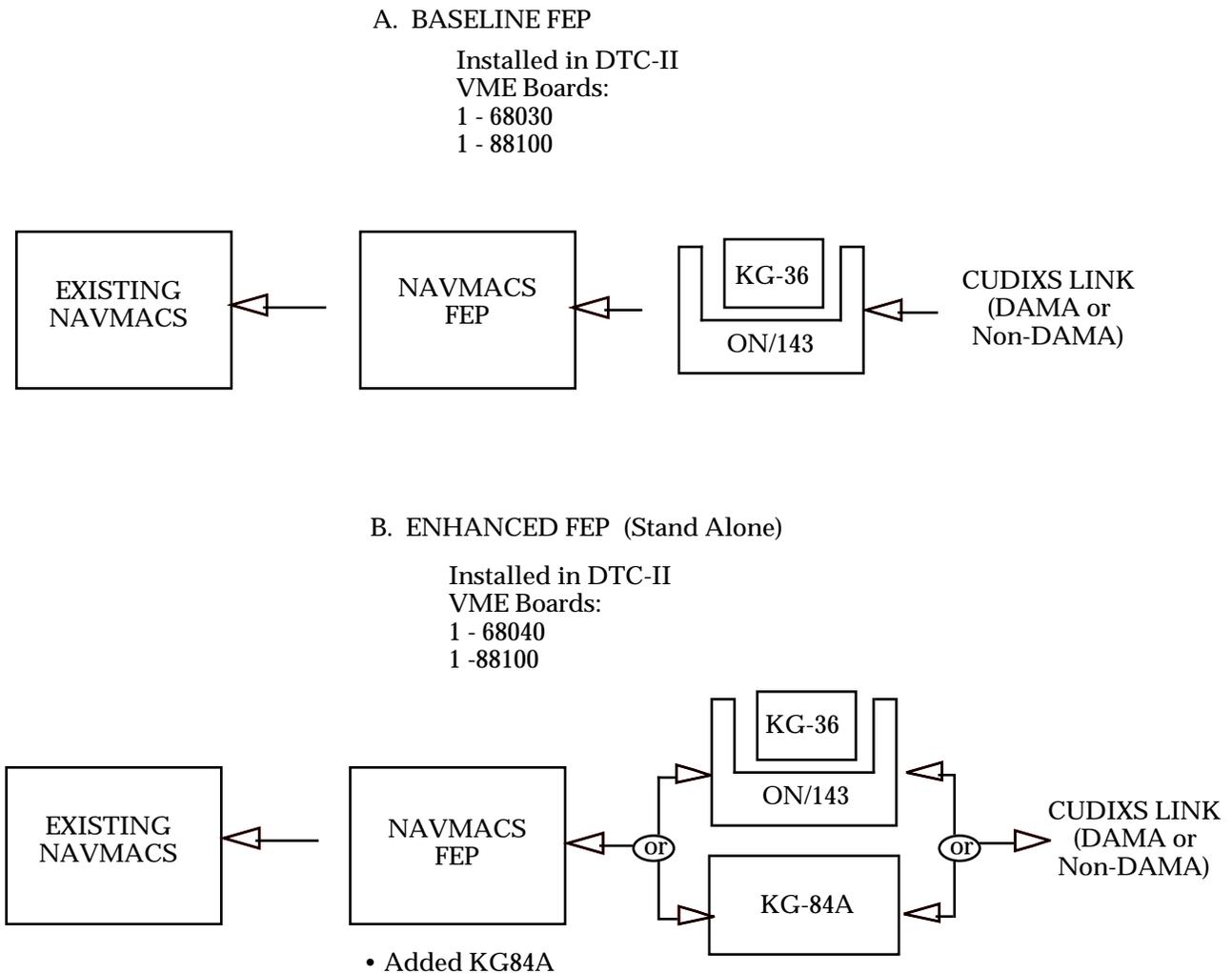


Figure 2. NAVMACS Front End Processor

The Message Processor (MP) segment performs all current NAVMACS user functions including message processing, map server/tactical presentation, and CC control. It is hosted on a DTC-II SPARC workstation and it interfaces to the users and to the Model II CC via an ethernet LAN.

The CSS SCE based CC segment provides the interfaces to multiple RF communication links and intelligently routes messages between the MP and these links. The CC is hosted in a separate VME chassis. The NAVMACS Model II CC VME board set includes one 68040 microprocessor, one 88100 microprocessor (used to run the modified FEP software), and three serial Input/Output (I/O) boards. The Model II CC software architecture includes Subscriber Interface Control and Resource Access Control. The host hardware for the CC consists of distributed Single Board Computers (SBCs) and workstations communicating over Ethernet and VME. Figure 3 illustrates the NAVMACS Model II, including the “embedded” FEP CC Subscriber Interface Control (SIC). The SIC interfaces to the MP for data exchange and flow control using a predefined set of interface message formats. The SIC receives message data from the MP and routes the data to the appropriate RF Link. In the NAVMACS-II implementation the routing is performed statically based upon an initialization table received from the MP.

A generic CSS SCE RAC is used in the CC. The RAC buffers message data and enforces flow control between the SIC and the Subnet Access Control (SAC). The RAC to SAC interface is a standard interface identical to that currently used in the Navy EHF Communication Controller (NECC). RF I/O circuits are handled by the RACs via individual serial I/O interfaces to the appropriate crypto. Up to 15 channels are provided for receipt of Fleet Broadcast channels (receive only) and other full duplex (e.g. UHF LOS or HF) links. The CC RAC assembles incoming data into data blocks based on the data type and rate for each link. These blocks of message data are labeled and passed back via the SIC to the message processing software, which does data conversions (e.g., Baudot-to-ASCII) and assembles the data blocks into discrete Navy messages.

A modified FEP software package is used in NAVMACS Model II as the CUDIXS SAC. The interface to the KG-36 or KG-84A (CUDIXS link) remains the same as for the FEP, but the FEP serial interface to an existing NAVMACS is replaced by a VME interface to a CC RAC.

NAVMACS
User Stations

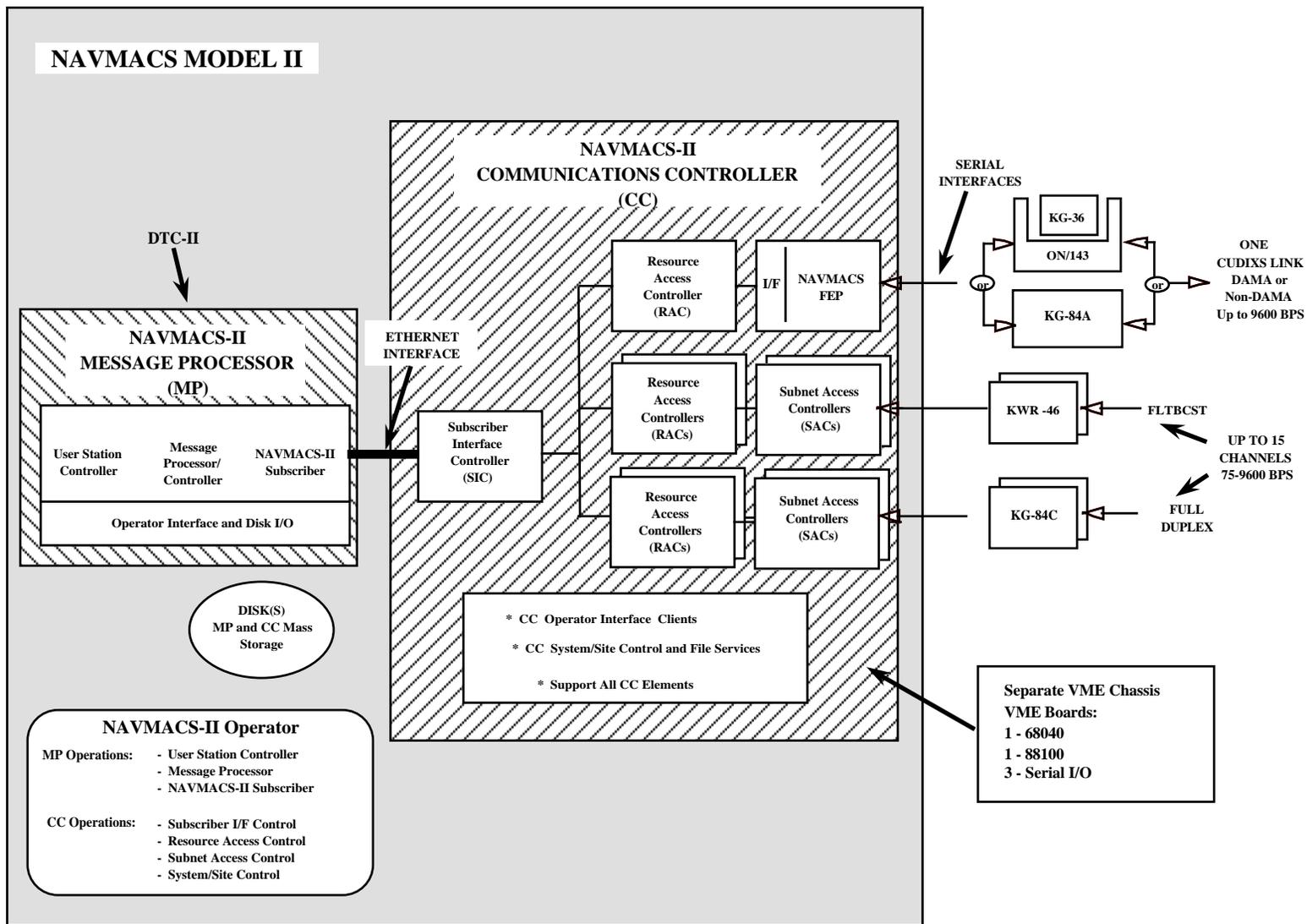


Figure 3. NAVMACS MODEL II

The Navy Extremely High Frequency (EHF) Communications Controller (NECC) project is currently in the process of fielding an SCE based system. This program has extensively developed the prototype SCE, adding further fault tolerance, improving the routing algorithms, and implementing COMPUSEC features. Figure 4 illustrates the architecture of the NECC.

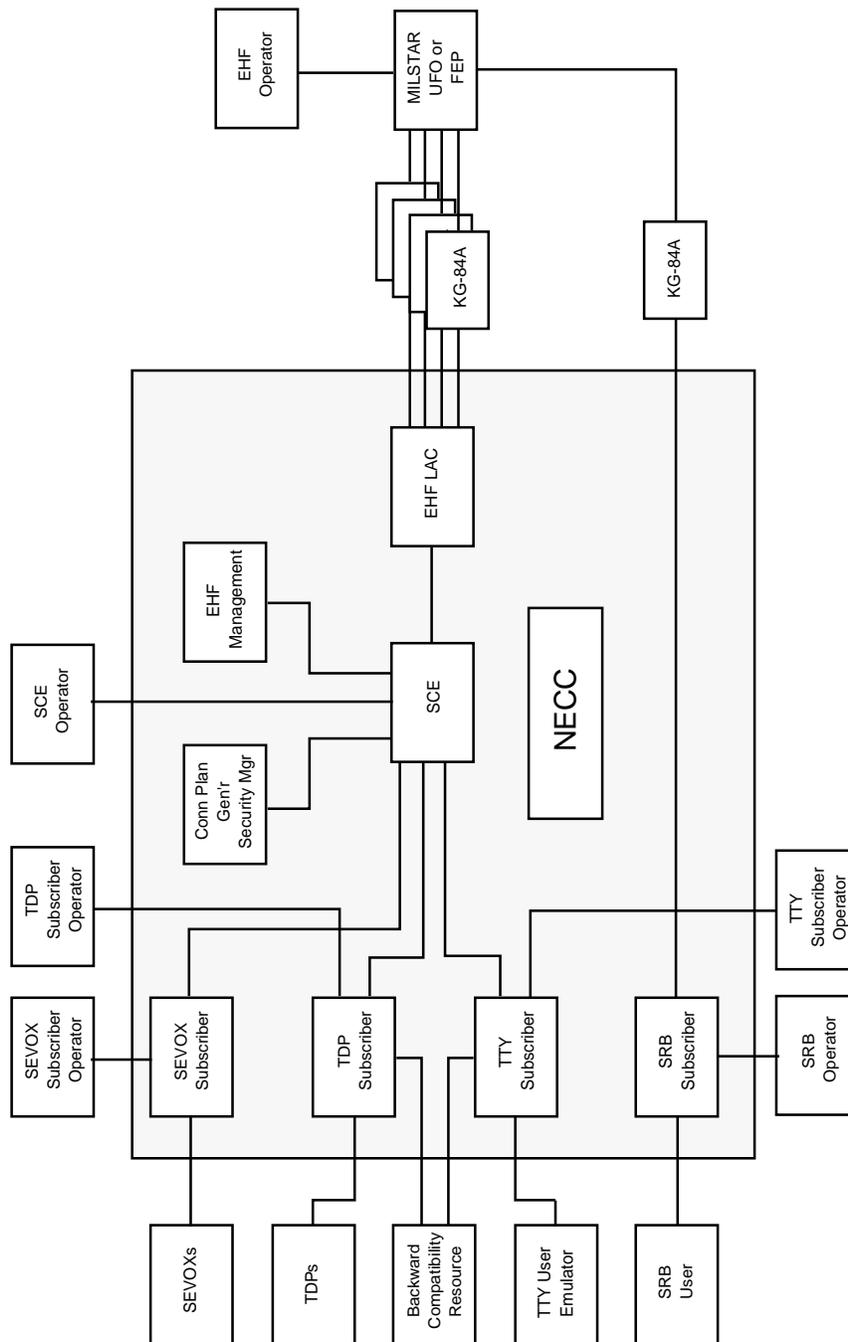


Figure 4. NECC Block Diagram

5.0 DEMONSTRATION CONFIGURATION

This section describes the system architecture of the intelligent gateway demonstrated for this contract. The ensuing discussion focuses on the functional components of the system which has been organized around specific hardware elements. As already discussed, the demonstration system architecture is based upon the prototype CSS SCE. Within the demonstration configuration, the gateway supports multiple user message types. Specifically, the gateway is capable of routing standard Transmission Control Protocol/Internet Protocol (TCP/IP) based internet data (e.g., E-Mail), Joint Operations Tactical System (JOTS) messages, and LINK-11 tactical data over multiple RF media. The prototype SCE based gateway in the demonstration configuration provides a multiband communications gateway between user traffic nodes and the RF media resources. A single layer of information security (INFOSEC) is implemented in this system through link level encryption. The demonstration configuration is illustrated in Figure 5.

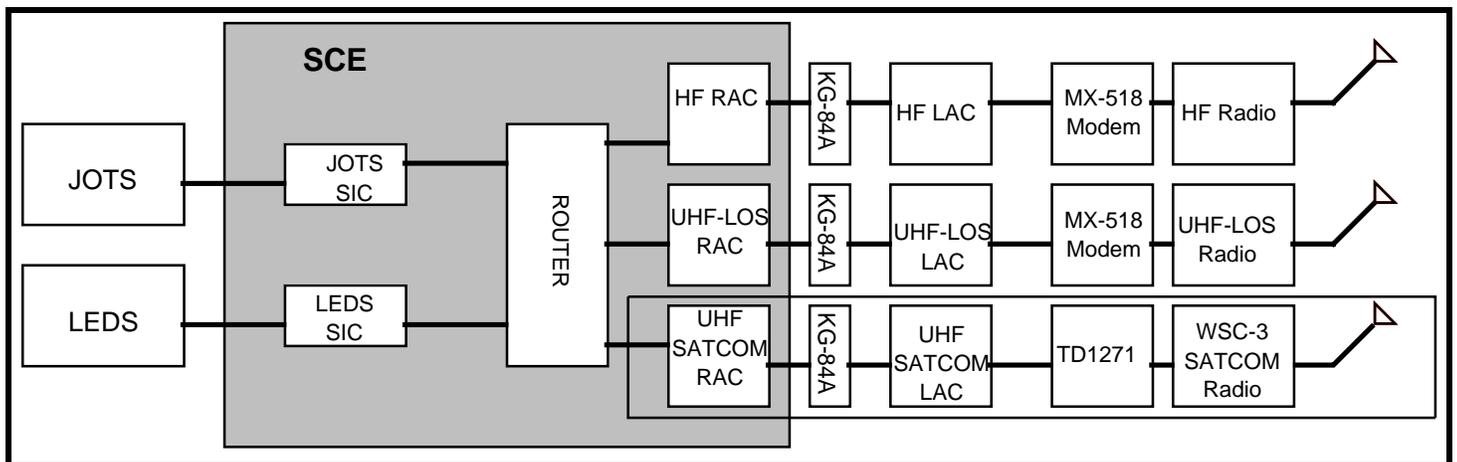


Figure 5. CSS SCE Demonstration Configuration

The various components of this demonstration system are briefly described in the following subparagraphs.

5.1 JOTS

The DTC-II hosted Joint Operational Tactical System (JOTS) provided the OTCIXS traffic for the demonstration.

5.2 LEDS

The LINK-11 Display System (LEDS) employs a simulcast/reception scheme to transparently monitor Combat Direction System (CDS) transmissions. It passes transmit opportunity buffers to the gateway (CSS SCE) for transfer over the RF media. Conversely, at the receiving end, it accepts data received over the RF media from the gateway and passes it onto the CDS.

5.3 Traffic Generator

The traffic generator hosted on the SPARC workstation was employed in the demonstration to generate the TCP/IP based internet traffic. The information generated by the traffic generator included *remote login*, *data file transfer*, *E-Mail*, and standard *network diagnostic* data (e.g., "ping").

5.4 Gateway Element (CSS SCE)

The Subscriber Interface Control (SIC), Router, and Resource Access Control (RAC) elements of the prototype CSS SCE were hosted in an individual "red" VME chassis. This gateway component interfaced to the JOTS and LEDS user components via, respectively, an IDS-8648 and X.25 computer-to-computer interfaces. The gateway interfaced to the link access elements hosted by a "black" VME chassis via KG-84A encryption devices. The implementation of the routing algorithm employed by the prototype CSS SCE is described in Appendix A (Prototype CSS SCE Routing Algorithm).

5.5 Link Access Elements

Two separate link access components were employed in the demonstration. These components were hosted in an individual "black" VME chassis. The Multi-User SATCOM for TDMA-1 (MUST) component was a UHF SATCOM link protocol which is a packet based attempt to optimize traffic throughput with minimal overall composite traffic delay. It manages allocation of transmission slots to users such that traffic load is optimally matched to current slot assignments in the link subnetwork.

The Minimum Coverage Approximation/Dynamic Hand-off Assigned Multiple Access (MINCAP/DHAMA) is a multiband networking protocol designed to allow multiple platforms (e.g., a U.S. Navy battle group) to access the composite capacity of multiple RF media (UHF-LOS and HF in the demonstration) through dynamic bandwidth management.

5.6 KG-84A

The KG-84A was used in the demonstration to provide single level link encryption. INFOSEC was implemented by KG-84A encryption/decryption of data at the RAC/LAC interface.

5.7 MX-518 Modem

The MX-518 is a single tone wave form modem. It utilizes an adaptive equalization signal processing scheme to coherently sum multiple HF propagation multipath components. The single tone waveform was adapted for TDMA in the demonstration by reducing the preamble time.

5.8 TD-1271

Two TD-1271 Demand Assigned Multiple Access (DAMA) channels were used in the demonstration by the MUST RAC. One low-rate channel was used by this RAC for transmission coordination at 600 bps. The second channel was used at 2400 bps for the actual data transfer.

6.0 DEMONSTRATION OVERVIEW

The intelligent gateway demonstration took place on February 1, 1995 in Building 660 at NRaD. The demonstration was scheduled to last 1 hour from 12:30 PM to 1:30PM. Due to time constraints caused by the COMMSYS 2000 meeting taking place concurrently at NRaD, the demonstration was accelerated and was given in approximately 35 minutes. The basic concept demonstrated was the automatic routing of messages over live RF links between identical communication equipment suites located within Building 660 and Building 15. These buildings are located near the Pacific Ocean shoreline near the U.S. Coast Guard Pt. Loma lighthouse. The building themselves are separated by approximately 300 feet.

Three independent sites were implemented for the demonstration. Two sites, located respectively in Building 15 and 660, were set up as both the source and destination sites for messages. At both sites, a Joint Operational Tactical System (JOTS) and Link-11 Display System (LEDS) message origination and destination user systems were interfaced to the intelligent gateway communications suite. A third site was also set up within Building 660. This site was implemented without any user systems. It contained only the intelligent gateway communications suite. Its role was to serve as a wide area internet relay - an intermediate node (site) between source and destination nodes (sites).

The purpose of the demonstration was to show (1) the automatic routing of messages over RF media without human intervention, (2) the automatic selection of RF media over which the message is to be transmitted, and (3) ability to transfer messages between two sites which are not

directly connected via an intermediary site. The three RF media set up for the demonstration were those employed by U.S. Coast Guard Cutters. These were UHF Line-of-Sight (LOS), UHF SATCOM, and HF. Due to UHF SATCOM equipment failure prior to demonstration, only the HF and UHF-LOS media were used for the demonstration. Furthermore, another problem occurred midway through the demonstration when a fault occurred within the core routing software in the intermediate relay site. Consequently, the ability to send messages between two sites incapable of direct RF communications via a relay site was not demonstrated.

For the short 35 minute demonstration, an operator in Building 15 entered commands at both the JOTS and LEDS systems to send messages continuously to Building 660. Without any human intervention, the intelligent gateway algorithm routed the message data to the RF resource it deemed optimal for the data transmission. Both LEDS track data and JOTS messages were transmitted over both UHF-LOS and HF media such that both media were equally utilized. This was done without any manual intervention. This multi-media routing operation implicitly demonstrated that a single RF media can be shared by multiple users. Finally, in order to demonstrate the significance of using the ISO layered protocol abstractions, particularly standard transport and network protocols such as TCP/IP, the standard UNIX "ping" message was generated at the traffic generator system in Building 660. Transparently and automatically, this information was received by the traffic generator system in Building 15 and a response was sent back to the traffic generator in Building 660. This was performed over both the HF and UHF-LOS media. The implication of this is the fact that in addition to tactical and non-tactical command and control systems on Coast Guard cutters, standard commercial communication applications can be run by users employing the intelligent gateway based communication system. These applications include standard electronic mail (E-Mail) and workstation utilities such as the "file transfer protocol" (ftp).

APPENDIX A

PROTOTYPE CSS SCE ROUTING ALGORITHM

The demonstration SCE permits multiple user messages to share use of one or more RF resources. Messages are allocated to one or more resources according to the active CSS COMMPLAN, henceforth referred to as CONNECTION PLAN in order to avoid confusion with the actual hardcopy Coast Guard COMMPLAN directive. The CONNECTION PLAN is a magnetic version of the COMMPLAN containing additional information such as:

- what destinations are reachable via each resource
- the "cost" of resource (e.g., UHF SATCOM should generally be more "expensive" than HF)
- the relative priority of each user's messages
- acceptable delivery time for user messages

The CONNECTION PLAN is a data base file selected at system initialization or upon command directives (i.e., new Coast Guard Cutter COMMPLAN) after the SCE-based communication system is operating. Messages from up to 16 users may be allocated to a single resource. Each user may be assigned to eight different resources. Transmit resources are selected (possible routing options) for each message from those resources that have been allocated to the specific user associated with the message. Resource Selection (routing) is performed for each message. The determination of a specific resource upon which to transmit the message, occurs according to the following selection process:

Step one: *User Identification* – The user associated with the message is identified.

Step two: *Resources Available.* – The available resources associated with the message is identified. An available resource is defined to be a resource that is allocated to the user associated with the message, and a resource that has the sufficient error rate, Low Probability of Intercept (LPI), anti-jam resistance, and Traffic Flow Security (TFS) attributes, and one which is accepting message data at the specified message precedence level.

Step three: *Transmit Address Evaluation* – From the message's destination address(es), the identities of all subnetworks servicing the resource set destination is identified. If resource sets cannot be identified that provide that connectivity to all addressees, and the "Best Effort Connectivity" Resource Selection option is NOT set in the CONNECTION PLAN for the user, an alert message is sent to the user via the user-SCE interface that the message has not been delivered. If the "Best Effort Connectivity" option is set, the user is informed via a status message of unreachable destinations. The output from this evaluation is a collection of candidate resource set(s).

Step four: *Acceptable Delivery Time* – Of the candidate resources remaining, those that do not permit the message to be delivered within the required delivery time are excluded as candidates. If there are no resources meeting the delivery requirements and the best effort delivery option is not enabled then the user is informed via a status message.

Step five: *Minimum Cost Resources* – Of the remaining candidate resources, the least number of resources are used. The resources having the least cost are selected over those with higher costs. The cost of a resource is specified in the active CONNECTION PLAN. If resources are not uniquely identified for selection, then that resource providing the most rapid delivery is selected.

The results of this process is the placement of message data in "user" queues for each resource selected for transmission.

APPENDIX B

ACRONYMS

BPS	Bits per Second
CC	Communication Controller
CDS	Combat Direction System
COMMPLAN	Communications Plan
COMPUSEC	Computer Security
COTS	Commercial-Off-the-Shelf
CSS	Communications Support System
CUDIXS	Common Digital User Information Exchange Subsystem
DAMA	Demand Assigned Multiple Access
DOD	Department of Defense
DTC	Desktop Computer
EHF	Extremely High Frequency
E-Mail	Electronic Mail
EMCON	Emission Control
EOC	Early Operational Capability
FEP	Front End Processor
	Fleet Satellite EHF Package (see fig. 4)
FLTSATCOM	Fleet Satellite Communications
FTP	File Transfer Protocol
GENSER	General Service
HF	High Frequency
INFOSEC	Information Security
ILS	Integrated Logistical Support
IP	Internet Protocol

ISO	International Standards Organization
IXS	Information Exchange System
JOTS	Joint Operational Tactical System
KG-36	Encryption/decryption equipment used with NAVMACS
KG-84A/C	Encryption/decryption equipment used with NAVMACS
kHz	kilo-Hertz
KWR-46	Encryption/decryption equipment used with NAVMACS
LAC	Link Access Control
LEDS	Link-11 Display System
LOS	Line of Sight
LPI	Low Probability of Intercept
MILSTAR	Military satellite constellation providing worldwide coverage
MINCAP/DHAMA	Minimum Coverage Approximation/Dynamic Hand-off Assigned Multiple Access
MM/DHAMA	Multi-Media Dynamic Hand-Off Assigned Multiple Access
MP	Message Processor
MUST	Multi-User SATCOM for TDMA-1
NAVMACS	Navy Modular Automated Communication System
NDI	Non-Developmental Item
NECC	Navy EHF Communications Controller
NRaD	Naval Command, Control and Ocean Surveillance Center, Research Development and Test Evaluation Division
ON-143	Red/black interface for KG-36
OSI	Open Systems Interconnection.
OTCIXS	Officer in Tactical Command Information Exchange Subsystem
RAC	Resource Access Control
R&D	Research and Development
RF	Radio Frequency

SAC	Subnet Access Control
SATCOM	Satellite Communications
SBC	Single Board Computer
SCE	Standard Communications Environment
SCSI	Small Computer System Interface
SHF	Super High Frequency
SIC	Subscriber Interface Control
SPARC	Scalable Processor Architecture
SRB	Submarine Report Back
STP	Software Test Plan
TADIXS	Tactical Data Information Exchange Subsystem
TCP	Transmission Control Protocol
TDP	Tactical Data Processor
TFS	Traffic Flow Security
TDMA	Time Division Multiple Access
TTY	Teletypewriter
UFO	UHF Follow-on
UHF	Ultra High Frequency
UHF LOS	UHF Line of Sight
VME	Versa Module Europa
X.25	The protocol which provides devices with direct connection to a packet switched network